PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 130, Number 3, Pages 653–659
S 0002-9939(01)06099-3
Article electronically published on August 29, 2001

SUBGROUP GROWTH IN SOME PRO-p GROUPS

YIFTACH BARNEA AND ROBERT GURALNICK

(Communicated by Lance W. Small)

Abstract. For a group G let $a_n(G)$ be the number of subgroups of index n and let $b_n(G)$ be the number of normal subgroups of index n. We show that $a_{p^k}(SL_2^1(\mathbb{F}_p[[t]])) \leq p^{k(k+5)/2}$ for $p > 2$. If $\Lambda = \mathbb{F}_p[[t]]$ and p does not divide d or if $\Lambda = \mathbb{Z}_p$ and $p \neq 2$ or $d \neq 2$, we show that for all k sufficiently large $b_{p^k}(SL_d^1(\Lambda)) = b_{p^{k+d^2-1}}(SL_d^1(\Lambda))$. On the other hand if $\Lambda = \mathbb{F}_p[[t]]$ and p divides d, then $b_n(SL_d^1(\Lambda))$ is not even bounded as a function of n.

1. Introduction

For a group G, let $a_n(G)$ be the number of subgroups of index n. Lubotzky and Mann [LM] proved that a pro-p group G is p-adic analytic if and only if it has polynomial subgroup growth; that is, there exists a constant c such that $a_n(G) \leq n^c$ (for background on p-adic analytic pro-p groups the reader is referred to [DDMS]). In [Sh, Corollary 2.5] Shalev proved the following:

Theorem 1.1. *Let G be a pro-p group which satisfies*
$$a_n(G) \leq n^{c \log_p n}$$
for some constant $c < \frac{1}{8}$. Then G is p-adic analytic.

Following this result Mann [Ma] asked the following:

Question. What is the supremum of the numbers c, such that if G is a pro-p group and $a_n(G) < n^{c \log_p n}$ for all large n, then G is p-adic analytic?

To continue our discussion we need the following definition.

Definition 1.1. Let Λ be a local ring with a maximal ideal M. We define the n-congruence subgroup of $SL_d(\Lambda)$ to be
$$SL_d^n(\Lambda) = \ker(SL_d(\Lambda) \to SL_d(\Lambda/M^n)).$$

The particular examples of local rings we deal with are $\Lambda = \mathbb{Z}_p$, the p-adic integers, and $M = p\mathbb{Z}_p$ or $\Lambda = \mathbb{F}_p[[t]]$, formal power series over a field of p-elements, and $M = t\mathbb{F}_p[[t]]$. It is well known that for these examples Λ, $SL_d^1(\Lambda)$ is a pro-p group. Moreover, $SL_d^1(\mathbb{F}_p[[t]])$ is not p-adic analytic. In [Sh] it is already shown that $a_{p^k}(SL_2^1(\mathbb{F}_p[[t]])) \leq Ap^{2k^2}$ for $p > 2$ and some constant A. We show the following:

Received by the editors March 1, 2000 and, in revised form, September 18, 2000.
2000 *Mathematics Subject Classification.* Primary 20E18; Secondary 17B70.
Both authors wish to thank MSRI for its hospitality. The second author was also partially supported by an NSF grant.

©2001 American Mathematical Society

Theorem 1.2. *Let $G = SL_2^1(\mathbb{F}_p[[t]])$ with $p > 2$. Then $a_{p^k}(G) \leq p^{k(k+5)/2}$.*

Thus in answer to Mann's question we show that the supremum is no more than $\frac{1}{2}$ (for $p > 2$).

We now turn our attention to the study of the lattice of normal subgroups of $SL_d^1(\Lambda)$, for $\Lambda = \mathbb{Z}_p$ and $\Lambda = \mathbb{F}_p[[t]]$. Let us recall that a group G is called **just infinite** if its only nontrivial normal subgroups are of finite index. It is well known that if $p \neq 2$ or $d \neq 2$, then $SL_d^1(\Lambda)$ is just infinite (this is actually shown in the proof of Lemma 4.1). In [Yo, Proposition 3.5.1] it is shown that the lattice of normal subgroups of another just infinite pro-p group, J_p, the Nottingham group is "periodic" ($p > 3$). In particular for any k, $b_{p^k}(J_p) = b_{p^{k+1}}(J_p)$. We show the following:

Theorem 1.3. *Suppose $\Lambda = \mathbb{F}_p[[t]]$ and p does not divide d or $\Lambda = \mathbb{Z}_p$ and $p \neq 2$ or $d \neq 2$. There is a constant $K = K(p, d)$ such that $b_{p^k}(SL_d^1(\Lambda)) = b_{p^{k+d^2-1}}(SL_d^1(\Lambda))$ for all $k > K$.*

Theorem 1.3 and the result for the Nottingham group might suggest that for any just infinite pro-p group a similar phenomenon occurs. The following theorem is thus somewhat surprising, as it shows that there is a big difference in the behavior of $b_n(SL_d^1(\mathbb{F}_p[[t]]))$ in the case p divides d.

Theorem 1.4. *If p divides d, then $b_n(SL_d^1(\mathbb{F}_p[[t]]))$ is not bounded as a function of n.*

Our main tool in this paper is Lie methods. It would be interesting to find a proof of Theorem 1.3 in the case $\Lambda = \mathbb{Z}_p$ based on powerful groups. This might help to handle the case where $p = d = 2$.

2. Lie methods

Suppose $\Lambda = \mathbb{Z}_p$ or $\Lambda = \mathbb{F}_p[[t]]$. Let $G_n = SL_d^n(\Lambda)$. It is straightforward to see that $(G_n, G_m) \subseteq G_{n+m}$ and $G_n^p \subseteq G_{n+1}$. Thus G_n/G_{n+1} is an elementary abelian p-group. It is easy to verify that $|G_n/G_{n+1}| = p^{d^2-1}$ and indeed this quotient is the adjoint module for $SL_d(\mathbb{F}_p)$.

The reader is referred to [LSh] for more details on the following construction. Define

$$L(G_1) = \sum G_n/G_{n+1}.$$

If $x \in G_n$ and $y \in G_m$, we define the bracket product

$$[xG_{n+1}, yG_{m+1}] = (x, y)G_{n+m+1}.$$

Extending this product by linearity gives $L(G_1)$ the structure of a Lie algebra over $\mathbb{F}_p$. It is not hard to check that $L(G_1) \cong t\mathfrak{sl}_d(\mathbb{F}_p)[t]$ — the set of polynomials with 0 constant coefficient over $\mathfrak{sl}_d(\mathbb{F}_p)$.

Let H be a closed subgroup of G_1. We define

$$L(H) = \sum (H \cap G_n)G_{n+1}/G_{n+1}.$$

The following facts are easy to verify:

1. $L(H)$ is graded subalgebra of $L(G_1)$.
2. If $K \leq H$ are closed subgroups, then $L(K) \subseteq L(H)$ and $\dim(L(H)/L(K)) = \log_p[H : K]$.

3. If H is normal, then $L(H)$ is an ideal.
4. $G_n \leq H$ if and only if $t^n \mathfrak{sl}_d(\mathbb{F}_p)[t] \subseteq L(H)$.
5. If $L(H)$ is generated by d homogeneous elements, then $d(H) \leq d$, where $d(H)$ is the minimal number of elements required to generate H topologically.

Let us remark that one can associate to the group G_1/G_n the Lie algebra $t\mathfrak{sl}_d(\mathbb{F}_p)[t]/(t^n)$. Similar results to the above holds for subgroups and subalgebras.

3. The subgroup growth of $SL_2^1(\mathbb{F}_p[[t]])$

We first consider a question about generation of Lie subalgebras of $L = t\mathfrak{sl}_2(\mathbb{F}_p)[t]/(t^{n+1})$. There should be an analogous result for other simple Lie algebras. Note that there exist Lie subalgebras of L which require the maximum number of generators given in the result.

Proposition 3.1. *Let $L = t\mathfrak{sl}_2(\mathbb{F}_p)[t]/(t^{n+1})$ with $p > 2$. If H is a graded subalgebra of L of dimension d and codimension c, then H can be generated by* $\min\{c+3, d\}$ *elements. In particular, H can be generated by no more than $\frac{3}{2}(n+1)$ homogeneous elements.*

Proof. First note that the second statement follows from the first since H can be generated by $(1/2)(c + d + 3) = (3/2)(n + 1)$ homogeneous elements.

Let $H = H_1 t \oplus \cdots \oplus H_n t^n$, where $H_i \subseteq \mathfrak{sl}_2(\mathbb{F}_p)$, and let $h_i = \dim H_i$. Similarly, let H_i' denote the degree i component of the derived algebra $[H, H]$ and set $h_i' = \dim H_i'$.

We recall that if M is a nilpotent Lie algebra and S is a subalgebra, then $S = M$ if and only if $S + [M, M] = M$ [Ja, Exercise I.10]. In particular, this implies that if M is a finite dimensional graded nilpotent Lie algebra, then M can be generated by $\dim(M/[M, M])$ homogeneous elements (of course, this is also the minimum number of generators required).

We also recall that $\mathfrak{sl}_2(\mathbb{F}_p)$ $(p > 2)$ is a simple Lie algebra and therefore a perfect Lie algebra, namely equals its derived subalgebra. Let V, U be subspaces of $\mathfrak{sl}_2(\mathbb{F}_p)$. As $\dim \mathfrak{sl}_2(\mathbb{F}_p) = 3$, it is easy to verify the following facts:

1. If $\dim V = 2$, then $[V, \mathfrak{sl}_2(\mathbb{F}_p)] = \mathfrak{sl}_2(\mathbb{F}_p)$.
2. If $\dim V = 1$, then $\dim[V, \mathfrak{sl}_2(\mathbb{F}_p)] = 2$.
3. If $\dim V = 2$, then $\dim[V, V] = 1$.
4. If $V \neq U$ and $\dim V = \dim U = 2$, then $[V, U] = \mathfrak{sl}_2(\mathbb{F}_p)$
5. If $\dim V = 2$ and $\dim U = 1$, then $1 \leq \dim[V, U] \leq 2$.

Of course, H can always be generated by d homogeneous elements.

We use an induction on n. For $n = 1, 2$, the result is clear. If $h_n' = 0$, then for all $1 \leq i < n$, $[H_i, H_{n-i}] \subseteq H_n'$; therefore $h_i + h_{n-i} \leq 3$. Thus, $c \geq (3/2)(n - 1)$ and $d \leq c + 3$. Note in fact this argument is valid under the weaker assumption that $h_i + h_{n-i} \leq 3$ for all $1 \leq i < n$.

So we assume that $h_i + h_{n-i} \geq 4$ for some i. Let j be the smallest positive integer such that $h_j + h_{n-j} \geq 4$.

If $h_i + h_{n-i} \geq 5$ for some i, then $h_n' = 3$. If $h_n' = 3$, then by induction $H/H_n t^n$ can be generated by at most $c + 3$ homogeneous elements. Since $H_n t^n \subseteq [H, H]$, this implies the same for H.

So we may assume that $h_i + h_{n-i} \leq 4$ for all i and that $h_n' \leq 2$.

Let Δ denote the set of integers with $h_i + h_{n-i} = 4$. Set $e = |\Delta|$. We notice that $d \leq 3 + (3/2)(n - 1) + e/2$ and $c \geq (3/2)(n - 1) - e/2$. Thus $d - e \leq c + 3$. Since j is minimal in Δ, $n - j$ is maximal in Δ and so $i + j \leq n$ for all $i \in \Delta$.

First suppose that $h_j \geq 2$. Then $[H_j t^j, H_i t^i] \neq 0$ for any $i \in \Delta$ and since these spaces are independent, it follows that $\dim[H,H] \geq e$. Thus, $\dim H/[H,H] \leq d - e \leq c + 3$ as required.

Finally, consider the case that $h_j = 1$ (and so $h_{n-j} = 3$ and $h'_n = 2$). Let $i \in \Delta$. So either $h_i = h_{n-i} = 2$ and $[H_j t^j, H_m t^m] \neq 0$ for $m = i, n-i$ or exactly one of h_i, h_{n-i} is 3. Thus, $[H_j t^j, \bigoplus_{i \in \Delta} H_i t^i]$ has dimension at least e. So $[H,H]$ has dimension at least e and as in the previous paragraph, we deduce that $\dim H/[H,H] \leq c+3$. $\square$

Proof of Theorem 1.2. Let $G_i = SL_2^i(\mathbb{F}_p[[t]])$. The G_i are a base for the neighborhoods of the identity. As G is finitely generated for any given k, there is m big enough such that G_m is contained in all subgroups of index p^k (actually Shalev [Sh, Theorem 4.1] proved that $m = k+1$ is sufficient). Therefore $a_{p^k}(G) = a_{p^k}(G/G_m)$. For any group H let $g_n(H)$ be the supremum on the number of generators of subgroups of index n. From [LSh, Lemma 4.1] we see that

$$a_{p^k}(G) = a_{p^k}(G/G_m) \leq p^{g_1(G/G_m) + g_p(G/G_m) + \cdots + g_{p^{k-1}}(G/G_m)}.$$

By fact 5 in Section 2, the remark following it and Proposition 3.1 we deduce that

$$a_{p^k}(G_1) \leq p^{0+1+2+\cdots+(k-1)+3k} = p^{k(k+5)/2}.$$

$\square$

4. The normal subgroup growth of $SL_d^1(\Lambda)$

Suppose $\Lambda = \mathbb{Z}_p$ or $\Lambda = \mathbb{F}_p[[t]]$. Let $G = SL_d^1(\Lambda)$ and $G_n = SL_d^n(\Lambda)$.

Lemma 4.1. *Suppose $\Lambda = \mathbb{F}_p[[t]]$ and p does not divide d or $\Lambda = \mathbb{Z}_p$ and $p \neq 2$ or $d \neq 2$. Then there is a constant $f = f(p,d)$ such that, for any normal subgroup N of G, there exists an n such that $G_{n+f} < N \leq G_n$.*

Proof. Let $\Lambda = \mathbb{F}_p[[t]]$ or $\Lambda = \mathbb{Z}_p$. Let n be maximal such that $N \leq G_n$. Therefore we can find $x \in N$ such that $x \notin G_{n+1}$. Passing to $L(N) = \sum_{i \geq 1} L_i t^i$, we can find a homogeneous element $\bar{x} t^n \in L(N)$, where $0 \neq \bar{x} \in \mathfrak{sl}_d(\mathbb{F}_p)$. Define $U_1 = [\bar{x}, \mathfrak{sl}_d(\mathbb{F}_p)]$ and by induction $U_{m+1} = [U_m, \mathfrak{sl}_d(\mathbb{F}_p)]$. Define $U = \bigcup U_m$. This is a nontrivial ideal of $\mathfrak{sl}_d(\mathbb{F}_p)$. If p does not divide d, then $\mathfrak{sl}_d(\mathbb{F}_p)$ is a simple Lie algebra. Therefore $U = \mathfrak{sl}_d(\mathbb{F}_p)$. As $\mathfrak{sl}_d(\mathbb{F}_p)$ is perfect, we see that $U_m \subseteq U_{m+1}$ for all m and moreover, equality holds if and only if $U_m = \mathfrak{sl}_d(\mathbb{F}_p)$. As $\dim(\mathfrak{sl}_d(\mathbb{F}_p)) = d^2 - 1$, we deduce that $U_{d^2-1} = \mathfrak{sl}_d(\mathbb{F}_p)$.

Since N is normal, $L(N)$ is an ideal and thus $[L(N), \mathfrak{sl}_d(\mathbb{F}_p)t] \subseteq L(N)$. Therefore $U_m \subseteq L_{n+m}$and $\mathfrak{sl}_d(\mathbb{F}_p) = L_{n+d^2+j-1}$ for $j = 0, 1, \ldots$. We now use fact 4 from section two to deduce that $G_{n+d^2-1} < N$.

Suppose now that $\Lambda = \mathbb{Z}_p$ and p divides $d > 2$. Let s be the largest positive integer such that p^s divides d. Since $p \neq 2$ or $d \neq 2$, $\mathfrak{sl}_d(\mathbb{F}_p)$ is perfect Lie algebra and its only non-trivial ideal is the center. Hence if U is not central, we can argue as above. Suppose that $\bar{x}$ is a scalar. Let $x = I + A$, where $A \in p^n M_d(\mathbb{Z}_p)$. As $\bar{x}$ is a scalar we can write $A = p^n \lambda I + B$, where λ is an invertible element of $\mathbb{Z}_p$, $B \in p^r M_d(\mathbb{Z}_p)$, $r > n$, and $B \bmod p^{r+1}$ is not a scalar. Hence we can write $x = (1 + p^n \lambda) I (I + C)$ where $C \in p^r M_d(\mathbb{Z}_p)$. We note that

$$\det((1 + p^n \lambda) I) = 1 + \sum_{i \geq 1} \binom{d}{i} p^{ni} \lambda^i.$$

Let t be maximal such that, for all $i \geq 1$, $\binom{d}{i}p^{ni} \bmod p^t \equiv 0$. We notice that when $n > s$, $t = n + s$. Hence $t - n$ is bounded by a function of p and d. As $1 = \det(x) = \det((1 + p^n\lambda)I)\det(I + C)$ and $\det((1 + p^n\lambda)I) \bmod p^{t+1} \not\equiv 0$, one can deduce that $C \bmod p^{t+1} \not\equiv 0$; moreover as p divides d, $C \bmod p^{t+1}$ is not a scalar.

It is not hard to find an element $y \in G$ which has the form $y = I + D$, where $D \in pM_d(\mathbb{Z}_p)$ and $[D, C] \bmod p^{t+2}$ is not a scalar. Set $z = (x, y) \in G_{t+1}$. We leave to the reader to verify that $z = I + E$, where $E \in p^{t+1}M_d(\mathbb{Z}_p)$, and $E \bmod p^{t+2} \equiv [D, C]$. From here the proof goes as in the case where p divides d, where we replace x by z, and noticing that $t + d^2 - n$ is bounded in terms of p and d. $\square$

Remarks. 1. The case where p does not divide d already appeared in an unpublished preprint by Aner Shalev.

2. In the course of the proof we actually showed that if $\Lambda = \mathbb{F}_p[[t]]$ and p does not divide d or $\Lambda = \mathbb{Z}_p$ and $p \neq 2$ or $d \neq 2$, then G is just infinite.

3. A similar argument to the case where $\Lambda = \mathbb{Z}_p$ and p divides d can be used to show that G is just infinite even when $\Lambda = \mathbb{F}_p[[t]]$ as long as $p \neq 2$ or $d \neq 2$.

We note that conjugation in G induces a structure of G-set on G_n/G_{n+d^2-1} for all n.

Lemma 4.2. *Suppose $\Lambda = \mathbb{F}_p[[t]]$ and p does not divide d or $\Lambda = \mathbb{Z}_p$ and $p \neq 2$ or $d \neq 2$. Let f be as in the previous lemma. Then there is one to one correspondence between the set of normal subgroups of G and the pairs (n, H) such that H is a subgroup of G_n/G_{n+f} which is not contained in G_{n-1}/G_{n+f} and H is G-invariant.*

Proof. Let N be a normal subgroup of G. By Lemma 4.1 we can find n such that $G_{n+f} < N \leq G_n$. We choose n to be maximal. Let $H = N/G_{n+f}$. Since n is maximal, H is not contained in G_{n-1}/G_{n+f}. As N is normal, H is G-invariant. On the other hand, given a pair (n, H), we take N to be the pre-image of H under the quotient map from G_n onto G_n/G_{n+f}. It is easy to verify that these maps are the inverses of each other. $\square$

Lemma 4.3. *Let f be some constant. Then for $n > f$ there is a map*

$$\varphi : G_n/G_{n+f} \to G_{n+1}/G_{n+f+1}$$

such that φ is an equivariant group isomorphism and

$$\varphi(G_{n+1}/G_{n+f}) = G_{n+2}/G_{n+f+1}.$$

Proof. First let us deal with the case $\Lambda = \mathbb{F}_p[[t]]$. Notice that every element of G_n has the form $I + A$, where $A \in t^nM_d(\mathbb{F}_p[[t]])$. We leave to the reader to check that if $n > f$, then the fact that the determinants of elements in G are one implies that $\mathrm{Trace}(A) \bmod t^{n+f} \equiv 0$. On the other hand if $\mathrm{Trace}(A) \bmod t^{n+f} \equiv 0$, then one can construct (using induction) an element in G_n of the above form.

We define a map

$$\varphi : G_n/G_{n+f} \to G_{n+1}/G_{n+f+1}.$$

By

$$\varphi((I + A)G_{n+f}) = (I + tA)G_{n+f+1}$$

(this is a slight abuse of notation as $I+tA$ does not necessarily have determinant 1). It is easy to check that φ satisfies the required conditions.

For $\Lambda = \mathbb{Z}_p$ the argument is very similar when we replace t by p. $\square$

Proof Theorem 1.3. Let f be as in Lemma 4.1. For $n > f$ we define $c(s)$ to be the number of G-invariant subgroups of G_n/G_{n+f} which are not contained in G_{n+1}/G_{n+f} and have index p^s. By Lemma 4.3 this is well defined and in particular does not depend on n.

Let us define $b_{k,n}(G)$ to be the number of normal subgroups of index p^k of G which contain G_{n+f} and are contained in G_n and n is maximal under this property. If H is a normal subgroup of index p^k, then by Lemma 4.1 there is n such that $G_{n+f} < H \le G_n$. We deduce that $p^{(n+f-1)(d^2-1)} > p^k \ge p^{(n-1)(d^2-1)}$; thus $\frac{k}{d^2-1}+1-f < n \le \frac{k}{d^2-1}+1$. We note that if $k > (2f-1)(d^2-1)$, then $n > f$.

By Lemma 4.2 and the above argument we see that for $n > f$ the following is true:

$$b_{k,n}(G) = \begin{cases} 0 & \text{if } n \le \frac{k}{d^2-1}+1-f, \\ 0 & \text{if } \frac{k}{d^2-1}+1 < n, \\ c(k-(n-1)(d^2-1)) & \text{otherwise.} \end{cases}$$

By Lemma 4.2 for $k > (2f-1)(d^2-1)$

$$b_{p^k}(G) = \sum_{n\ge 1} b_{k,n}(G) = \sum_{\frac{k}{d^2-1}+1-f<n\le\frac{k}{d^2-1}+1} c(k-(n-1)(d^2-1)).$$

Thus $b_{p^k}(G)$ depends only on $k \bmod d^2-1$ for $k > (2f-1)(d^2-1)$. $\square$

Proof of Theorem 1.4. We note that G_n/G_{2n} is an elementary abelian p-group; moreover G_n/G_{2n} is a G-module. Let $x \in G_n$ and let us write $x = I + A$, where $A \in t^n M_d(\mathbb{F}_p[[t]])$. We note that $\det(x) = 1$ implies that $\mathrm{Trace}(A) \bmod t^{2n} \equiv 0$. On the other hand suppose $\mathrm{Trace}(A) \bmod t^{2n} \equiv 0$; then one can construct (using induction) an element in G_n of the above form. As p divides d if $A \bmod t^{2n}$ is a scalar, then $\mathrm{Trace}(A) \bmod t^{2n} \equiv 0$. We also note that if $A \bmod t^{2n}$ is a scalar, then G acts trivially on $\langle xG_{2n}\rangle$. Let N_x be the pre-image of $\langle xG_{2n}\rangle$ in G_n. This is a normal subgroup of G of index $p^{(2n-1)(d^2-1)-1}$. Of course the number of such subgroups is equal to the number of $A \in t^n M_d(\mathbb{F}_p[[t]])$ such that $A \bmod t^{2n}$ are nonzero scalars divided by $p-1$. Therefore $b_{p^{(2n-1)(d^2-1)-1}}(G) \ge (p^n-1)/(p-1)$. $\square$

Acknowledgments

The authors would like to thank Dan Segal for his careful reading of an earlier version and some helpful comments.

References

[DDMS] J. Dixon, M.P.F. Du Sautoy, A. Mann and D. Segal, *Analytic Pro-p Groups*, 2nd edition, Cambridge Studies in Advanced Math. **61**, Cambridge University Press, Cambridge, 1999. MR **2000m:**20039

[Ja] N. Jacobson, *Lie Algebras*, Interscience, New York, 1962. MR **26:**1345

[LM] A. Lubotzky and A. Mann, Powerful p-groups. I, II. *J. of Algebra* **105** (1987), 484–515. MR **88f:**20045; MR **88f:**20046

[LSh] A. Lubotzky and A. Shalev, On some Λ-analytic pro-p groups, *Israel J. Math.* **85** (1994), 307–337. MR **95f:**20047

[Ma] A. Mann, Subgroup growth in pro-p groups, in *New Horizons in Pro-p Groups*, eds: M. du Sautoy et al., Progress in Mathematics 184, Birkhäuser, Boston, 2000, pp. 233–247. CMP 2000:15

[Sh] A. Shalev, Growth functions, p-adic analytic groups, and groups of finite coclass, *J. London Math. Soc.* **46** (1992), 111–122. MR **94a:**20047

[Yo] I.O. York, *The Group of Formal Power Series under Substitution*, Ph.D. Thesis, Nottingham, 1990.

Department of Mathematics, University of Wisconsin, 480 Lincoln Drive, Madison, Wisconsin 53706

E-mail address: `barnea@math.wisc.edu`

Department of Mathematics, University of Southern California, Los Angeles, California 90089-1113

E-mail address: `guralnic@math.usc.edu`